Daily Bulletin

November 7, 2003

Information Technologies Critical to Achieving Development Goals

U.S. diplomat says WSIS will focus on development needs

The following article by Ambassador David A. Gross, U.S. coordinator for International Communications and Information Policy, appears in the International Information Program Electronic Journal "The Evolving Internet" issued in November 2003.

This article and the rest of the journal may be viewed on the Web at:
http://usinfo.state.gov/journals/itgic/1103/ijge/ijge1103.htm.
No republication restrictions.

The Digital Dimension of Development: A Strategic Approach By Ambassador David Gross

(A top U.S. diplomat says the freedom to innovate, create, and share ideas is critical to development. He describes how the U.S. government is utilizing information and communications technology to achieve development goals.)

"In the new century, growth will be based on information and opportunity. Information drives markets, ensures a rapid reaction to health crises like SARS, and brings new entrepreneurial opportunities to societies....The keys to prosperity in an information economy are education, individual creativity, and an environment of political and economic freedom. An environment of economic and political freedom is

United States Mission, Office of Public Affairs, 11 Route de Pregny, 1292 Chambésy

Available on the Internet at: www.usmission.ch

the sina qua non for the kind of progress we are talking about."
-- Secretary of State Colin L.Powell before the World Economic Forum June 22, 2003

Over the past decade, breathtaking advances in information and communications technology (ICT) have changed the way we live, learn, and do business.

Whether it is responding more rapidly to health crises like SARS (severe acute respiratory syndrome), delivering education to the underserved, increasing government transparency, or creating new forms of commerce, technology is transforming our world.

ICT has become the new tool for achieving economic and social development. In fact, a growing global consensus has emerged in recent years that information-based technologies are fundamental to meeting basic development objectives.

The future prosperity and well being of all nations, including the United States, now depend in part on our ability to access and use these new tools effectively.

For much of the world, however, that remains an elusive goal. The number of Internet users in the world today exceeds 500 million but some 40 percent of that number live in the United States. Over the past 10 years, global telephone penetration rates have doubled, but there are still more telephone landlines in New York City's borough of Manhattan than in all of Africa. On the other hand, technology is dramatically changing things almost everywhere -- for example, there are now many more wireless phones in Africa than traditional landline phones.

World Summit on the Information Society

The upcoming United Nations World Summit on the Information Society (WSIS), scheduled for December 10-12 in Geneva, will focus precisely on these challenges.

The summit, the latest in a series of U.N. summits focused on development, will be attended by more than 50 heads of state and government from around the world. A second phase of the summit will be held in Tunis, November 16-18, 2005. Leaders from business, civil society, and international organizations are contributing to preparations for both phases.

The summit's mission is to outline a clear vision and a concrete plan for putting ICT into the service of development.
What considerations should guide the Summit's work?

Development begins with freedom. The freedom to innovate, the freedom to create, and the freedom to share ideas with people around the world are the foundation of a global, inclusive information society. Our overriding vision for the information society is one that expands political and economic freedom by offering our citizens the opportunities to access and utilize information to better their lives.

More specifically, we believe success in making freedom possible and crafting an ICT-for-development agenda depends on three fundamental building blocks.

A Strategic Approach

First, we believe countries should focus on creating a domestic policy environment that encourages privatization, competition, and liberalization, and that protects intellectual property.

Private investment is by far the largest source of funds for the development, deployment, maintenance, and modernization of the world's communications and information networks and facilities. Public policies that do not actively invite such investment simply delay development.

Around the world, there are encouraging signs that rules favoring competition are paying big dividends. In Uganda, for example, a price war broke out last year in the country's competitive telecommunications sector. Costs per minute for telephone calls tumbled and some firms scrapped fees. The result has been more opportunities for entrepreneurs and cheaper rates for all users.

Second, it is critical to build human capacity. Users must have the ability to effectively use ICT tools. Without adequate education and training, infrastructure investments will yield little.

Teachers, school children, health professionals, citizens, and business people must have the knowledge needed to take full advantage of distance learning, e-healthcare, e-government, and e-business applications.

To be used effectively, ICT tools also must be adapted to local needs. Local content that re ects local culture and is in the language of the users' choosing is vital to sus-

taining the effective use of ICT. The U.S. government believes such content should be widely available. At the same time, content restrictions must be avoided. Uncensored print and broadcast media provide independent and objective information and offer a vehicle for citizens to openly and freely express their opinions and ideas.

Artificial barriers that unnecessarily restrict the free ow of information and news are the enemies of innovation, retard the creation of knowledge, and inhibit the exchange of ideas that are necessary for people to improve their lives.

The realization of the many "digital opportunities" that ICT tools make possible depends on access to information. Electronic government, for example, can increase government transparency, accountability, and accessibility and lead to better development decisions as long as governments are prepared to share information with their citizens.

Third, users must be able to use ICT with confidence if the economic and social benefits of these technologies are to be achieved. Network security ICT tools and networks can never be made invulnerable to attack. But countries can protect their ICT infrastructure by adopting effective substantive and procedural laws.

Companies, consumers, and citizens can contribute as well by raising awareness and implementing widely recognized network security guidelines compiled by the United States and its partners in the Organization for Economic Cooperation and Development. Together we can create a global culture of network security that protects all users, no matter where they live.

In addition to creating the right policy environment, building human capacity, and protecting networks, governments also must avoid erecting new hurdles that will undermine efforts to harness ICT to development goals.

Whether it is weakening intellectual property protections, limiting press freedoms, or injecting governments unnecessarily into the technical management of the Internet, such misguided steps can quickly reduce choice, sti e innovation and democracy, and raise costs.

Partnerships for Development

The U.S. government's involvement in WSIS is only one aspect of our commitment to using ICT to foster development. Over the years, many of our assistance programs have incorporated ICT to achieve economic and social goals.

The Digital Freedom Initiative (DFI) is one of the leading examples of the U.S. government's (USG's) commitment to using the latest tools to achieve longstanding development goals. The program builds on previous USG initiatives, including the Leland Initiative, which was launched in 1996, and the Internet for Economic Development, which was launched in 1999.

The DFI promotes the use of ICT by entrepreneurs and small businesses in developing countries and leverages existing infrastructure to improve access to local, regional, and global markets. It also assists countries in creating a pro-competition policy and regulatory environment that will help entrepreneurship blossom.

The pilot program was announced in March 2003 at a White House ceremony and was first launched in Senegal. At the October 20-21 Asia-Pacific Economic Cooperation (APEC) Leaders Meeting in Bangkok, President Bush announced that Peru and Indonesia would join the program.

Over the next five years as many as a dozen countries may be invited to join the initiative.

The U.S. government advances ICT-for-development through numerous other programs. These include:

-- Literally hundreds of individual U.S. Agency for International Development projects that use ICT to address health, education, and capacity issues;

-- State Department-sponsored "e-logistics" workshops that provide practical real-world advice to developing country business owners, especially small and middle size enterprises eager to improve productivity and expand into new markets;

-- Regulatory and technical training programs sponsored by the U.S. Telecommunications Training Institute, which, over the past 20 years, has graduated more than 6,200 ICT professionals from 163 developing countries; and,

-- A $30 million Internet Access and Training Program (IATP) that develops Internet skills and computer knowledge among diverse populations in Eurasia while promoting the free ow of information and ideas.

Whether it is these programs, a new initiative to promote the spread of wireless technologies, or efforts to raise awareness about the value of "electronic government," all our ICT-for-development programs rest on the building blocks outlined above.

We believe that these building blocks can help all countries achieve their digital progress and prosperity agendas, thereby helping the children and generations to come.

Microsoft Works with U.S. Law Enforcement to Catch Cybercriminals

Software corporation offers rewards for information on malicious code incidents

Microsoft Corporation and U.S. law enforcement agencies are joining forces to step up the international pursuit of those responsible for the release of malicious computer code on the Internet. Microsoft is funding a $5 million reward program to support U.S. and international law enforcement in solving these episodes of cybercrime. The company November 5 announced that it is offering $250,000 rewards for information leading to the arrest and conviction of those who released the MSBlast.A computer worm and the SoBig virus earlier this year.

Malicious codes exploit vulnerabilities in Microsoft software by entering computers loaded with the software and performing operations not authorized by the computer owner. Experts estimate that corporations with computer systems infected by MSBlast.A starting in August 2003 spent more than $500 million to eliminate it, regain control of their equipment and restore lost data. Damages attributed to SoBig, which first appeared in January 2003, may approach $1,000 million, according to the CERT/Coordination Center, a federally supported agency monitoring computer security incidents.

"These are not just Internet crimes, cybercrimes or virtual crimes," said Brad Smith, senior vice president and general counsel at Microsoft in a news release issued jointly by the Microsoft and the U.S. Secret Service. "These are real crimes that hurt a lot of people. Those who release viruses on the Internet are the saboteurs of cyberspace, and Microsoft wants to help the authorities catch them,"

Representatives of the U.S. Secret Service, the Federal Bureau of Investigation and Interpol joined Microsoft representatives in the November 5 Washington news conference where the reward program was announced. Acting Deputy Assistant Director of the FBI's Cyber Division Keith Lourdeau emphasized the seriousness of the crimes, explaining that his agency is engaged in a partnership with industry to track down those who are releasing Blaster and other malicious code.

"To date, subjects have been charged and arrested in connection with the release of three of the six Blaster variants. While this is a sign of progress, the FBI will continue in its pursuit of the original authors of these worms," said Lourdeau in a separate statement.

Further information about Microsoft's reward program is available at HYPERLINK

"http://www.microsoft.com/presspass/features/2003/nov03/11-05AntiVirusQA.asp"

Further information about viruses and malicious codes is available at HYPERLINK

http://www.cert.org/other_sources/viruses.html"

Following is the text of the Microsoft-Secret Service announcement:

Nov. 5, 2003 Microsoft Announces Anti-Virus Reward Program

Microsoft Teams With Law Enforcement to Root Out Malicious Code Distributors With $5 Million Reward Fund as a Part of Broader Security Initiative

WASHINGTON -- Nov. 5, 2003 -- Microsoft Corp. today announced the creation of the Anti-Virus Reward Program, initially funded with $5 million (U.S.), to help law enforcement agencies identify and bring to justice those who illegally release damaging worms, viruses and other types of malicious code on the Internet. Microsoft will provide the monetary rewards for information resulting in the arrest and conviction of those responsible for launching malicious viruses and worms on the Internet. Residents of any country are eligible for the reward,

according to the laws of that country, because Internet viruses affect the Internet community worldwide.

As part of the Reward Program, Microsoft announced the first reward in the amount of a quarter-million dollars (U.S.) for information leading to the arrest and conviction of those responsible for unleashing the MSBlast.A worm. Although two arrests were made in connection with the B and C variants of the MSBlast worm, those responsible for releasing the original worm this summer remain at large. The worm was designed to attack Microsoft's www.windowsupdate.com Web site, which provides fixes for vulnerabilities and helps protect users against malicious attacks. Microsoft offered a second quarter-million-dollar reward for information that results in the arrest and conviction of those responsible for unleashing the Sobig virus. This virus, the first variant of which was detected Jan. 10, 2003, attacked individual machines and e-mailed itself to each e-mail address in the computer's contact list. The Sobig.B and Sobig.C variants of the virus made messages appear as if they had come from official Microsoft e-mail addresses. No arrests have been made in connection with the Sobig virus.

"Malicious worms and viruses are criminal attacks on everyone who uses the Internet," said Brad Smith, senior vice president and general counsel at Microsoft. "Even as we work to make software more secure and educate users on how to protect themselves, we are also working to stamp out the criminal behavior that causes this problem. These are not just Internet crimes, cybercrimes or virtual crimes. These are real crimes that hurt a lot of people. Those who release viruses on the Internet are the saboteurs of cyberspace, and Microsoft wants to help the authorities catch them."

Partnership Program With Law Enforcement

Representatives of three law enforcement agencies, the Federal Bureau of Investigation (FBI), the Secret Service and Interpol, today joined Microsoft at the National Press Club news conference, where the company provided details of the reward program.

"The malicious distribution of worms and viruses, such as MSBlast and Sobig, are far from victimless crimes," said Keith Lourdeau, Acting Deputy Assistant Director of the FBI Cyber Division. "Such attacks on the Internet cost businesses worldwide millions -- some estimates claim billions -- of dollars and wreak havoc on individuals by ruining files, hard drives and other critical data. We intend to vigorously pursue the perpetrators of these crimes, and we hope to see additional industry-government collaboration to identify these individuals."

"Not only are we concerned with apprehending those individuals who commit computer crimes but also in limiting the damage done by these criminals to private industry and the public," said Bruce Townsend, deputy assistant director of investigations at the Secret Service. "By working together, the public, the private sector and law enforcement can combine their resources to effectively combat computer-based crimes like the MSBlast.A worm and Sobig virus."

"Interpol is particularly interested in fighting the malicious spreading of viruses because this represents truly borderless crime that requires a truly global response, a global collaboration between police and private industry," said Interpol Secretary General Ronald K. Noble, at the organization's headquarters in Lyon. "This Microsoft reward program is an opportunity to continue building effective relationships between the world's police and the private sector in order to prevent and prosecute cybercrime."

Individuals with information about the MSBlast.A worm or the Sobig virus, or any other worms or viruses, should contact the following international law enforcement agencies:

-- International/Interpol: via the Interpol National Central Bureau in any of Interpol's 181 member countries or at http://www.interpol.int/

-- FBI or Secret Service: via any local field office

-- The Internet Fraud Comp laint Center: at http: //www.ifccfbi.gov/ Microsoft has made security a top priority and is committed to developing the most secure software possible and making it easier for customers to protect themselves against attacks launched by malicious law breakers. Over the past year, the company delayed several product development projects to provide intensive training for more than 18,000 developers on how to write more secure code. The company has taken numerous steps to alert users to possible vulnerabilities and steps they can take to protect themselves, including the recent "Protect Your PC" campaign. This information is available at http://www.microsoft.com/protect/. While working hard to improve the security of its software, Microsoft also cooperates with international, federal and state law enforcement to help bring the perpetrators of these attacks to justice.

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software -- any time, any place and on any device.

U.S. Provides Iraq's Mosul University with Computers and Internet Access

USAID works with Coalition Provisional Authority to rebuild Iraq

This article by Ben Barber, a writer for the U.S. Agency for International Development, was first published September 29, during a visit to Iraq. The article is in the public domain with no restrictions on republication.

For more information on U.S. efforts to rebuild Iraq, please visit the USAID website:

http://www.usaid.gov/iraq

U.S. Provides Iraq's Mosul University with Computers and Internet Access By Ben Barber USAID Staff Writer

MOSUL, Iraq -- After looters stole the computers at Mosul University and burned the computer center, students and teachers had no way to do research and communicate with colleagues around the country and the world.

USAID officials discovered the need and provided 48 computers along with Internet access in June, giving the university's 32,000 students a place to continue their studies.

Professor Wafa Al-Abidin, 35, was one of about 30 women and men working at the computers this morning, and her topic of study was modern women's poetry in the United States.

Each student or teacher can sign up to use the computer center for two hours a week. Although there are no printers yet, Dr. Al-Abidin downloads materials she finds on the Internet to oppy disks and takes them home where she has a computer and printer -- but no Internet.

"About two months ago the computers were installed. It was a good achievement for the Americans to set it up. The Internet is important for our work," she said.

"If there were three times as many computers here at school, they would be used," she said, asking also for a chance to visit America and for American professors to visit Iraqi universities to teach.

She shows a letter she received from the American poet Adrienne Rich -- "a Jew but she is my friend" -- offering to send her latest book of poems to the Iraqi professor.

Using the U.S.-provided computers and Internet access, Dr. Al-Abidin is able to download poetry and information and send e-mails to other researchers and to poets.

The $69,000 for computers and $74,000 for Internet access was provided by USAID working in cooperation with the Coalition Provisional Authority.

Abraham Urges U.N. to Confront Nonproliferation Challenges

U.S. energy secretary proposes three-pronged response

Energy Secretary Spencer Abraham told the United Nations November 5 that the maintenance and strengthening of the existing international nuclear nonproliferation regime requires finding ways to build on the successes of the past while overcoming the challenges of the present.

Addressing the U.N. First Committee on Disarmament and International Security, Abraham proposed three responses to today's nonproliferation challenges. First, he said, "concrete, achievable steps" must be taken to "enhance and improve traditional nonproliferation measures."

He said such steps should include:

-- strengthening safeguards, such as adopting the International Atomic Energy Agency's (IAEA's) Additional Protocol;
-- strengthening roadblocks to trafficking in nuclear and radiological materials and technologies for weapons purposes; and
-- strengthening the security of research reactors or other

facilities having nuclear and non-nuclear radiological material.

The second response, he said, would require addressing the "fundamental challenges to the nonproliferation regime." He focused his remarks particularly on Iran, noting that Tehran recently agreed to IAEA demands to take steps to meet its obligations under the Nuclear Non-Proliferation Treaty (NPT).

"If Iran carries out the obligations it has undertaken -- especially if it abandons its enrichment and reprocessing activities -- it will show what can be achieved when the international community sends the same firm message on the need to comply with nonproliferation requirements," Abraham said.

However, vigilance is necessa ry, Abraham said, in order to assure that Iran's promise is kept. He said Iran must:

-- Make full declaration of all imported material and components related to uranium enrichment;

-- Allow unrestricted access, including environmental sampling, for the IAEA to locations the IAEA requires;

-- Resolve all questions about uranium enrichment centrifuge testing;

-- Divulge complete information on uranium conversion experiments; and

-- Provide "such other information, explanations, or action that the IAEA deems necessary."

His third proposal is to "reconceptualize" underlying long-term security relationships. Abraham sees several steps as being necessary in this process:

-- First, he said, "we must reinforce the nuclear proliferation risks" run by those states acquiring enrichment and reprocessing capabilities. Possession of these capacities in the hands of states with "questionable commitments to the NPT" should automatically raise a warning sign and should be discouraged, he said.

-- Second, Abraham called for strengthening IAEA safeguards against "indigenous enrichment or reprocessing that could support illegitimate and proscribed activities." Beyond the IAEA Additional Protocol, he said, "[w]e should look for ways to ensure that the IAEA has the tools it needs to effectively address the problem posed by a state like North Korea, before such a state announces it has established a nuclear weapons capability."

-- Finally, Abraham suggested that it might be necessary "to think about new approaches to the fuel cycle that strictly limit the use of enrichment and reprocessing and access to nuclear weapons technology ... while ensuring that nuclear medicine, agriculture, energy supplies, and other critical benefits can be enjoyed in all responsible nations."

Please Note: Most texts and transcripts mentioned in the U.S. Mission Daily Bulletin are available via our homepage **www.usmission.ch**.
Select "Washington File" from the drop-down menu under "News."